The NMCI Experience and Lessons Learned

The Consolidation of Networks by Outsourcing

Case Studies in National Security Transformation
Number 12
Kenneth Jordan

Sponsored by the Office of the Deputy Assistant Secretary of Defense
Forces Transformation and Resources

Prepared by the Center for Technology and National Security Policy

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The NMCI Experience and Lessons Learned. The Consolidation of Networks by Outsourcing	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,BG 20, Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**15**	

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

Dr. Kenneth L. Jordan is a consultant to the Center for Technology and National Security Policy. His specialty is information and communications technology. He also supports the Office of Naval Research in determining research priorities to support Network Centric Warfare. He has been a Corporate Vice President of SAIC and has worked in the Office of the Secretary of Defense and the Office of the Secretary of the Air Force. He has an Sc.D. in Electrical Engineering from Massachusetts Institute of Technology.

Introduction

The Navy/Marine Corps Intranet (NMCI) has been an initiative to provide a single, secure, enterprise-wide network to support the naval shore establishment and tie it to the forces at sea by interfacing with the at-sea network. The plan has been to link 360,000 desktops into one seamless and secure intranet, sharing voice, video, and data services. It is an $8.8B performance-based services contract with Electronic Data Systems (EDS), initially awarded in October 2000. The scale of NMCI as an information network is second only to the internet itself, clearly an enormous effort.

NMCI has replaced the fractionated legacy[1] networks of the Navy and Marines with a secure, single, shore-based network. Since its inception, however, the program has been beset with problems. Delays in the fielding of the network have resulted in substantial financial losses for EDS. Customer satisfaction, upon which payments to the contractor depend, has not been uniformly high. Operational users feel that the centralized support approach provides them with less than satisfactory responsiveness in resolving network issues in support of operational situations. The main question is does this network provide sufficient performance to support the net-centric operational needs of the Navy and Marine Corps?

In this case study, we will investigate these issues and provide some lessons learned to support the future evolution of NMCI as well as other military networks.

Sources

In carrying out this case study, the author reviewed many publicly available articles, briefings, and congressional testimony concerning the NMCI program. Some of these references are available on the internet, and where possible, URLs that were valid as of the date specified are provided in the References section. The author also had informal discussions[2] with personnel involved in the requirements process for the Next Generation NMCI. Two references in particular are worth pointing out, one is the December 2006 Government Accountability Office (GAO) report entitled "DoD Needs to Ensure That Navy Marine Corps Intranet Program is Meeting Goals and Satisfying Customers;"[3] the other is a June 2005 article from *Government Computer News* entitled "Other agencies could benefit from NMCI's hard-learned lessons."[4]

---

[1] The term "legacy applications" refers to those applications that were in use by the different commands before NMCI.
[2] Chris Rigano, ONR Code 31 MITRE support, personal communication, 16 Mar. 2007.
[3] U.S. Government Accountability Office, DoD Needs to Ensure That Navy Marine Corps Intranet Program Is Meeting Goals and Satisfying Customers, GAO-07-51, Dec. 2006, <http://www.gao.gov/new.items/d0751.pdf>.
[4] Dawn S. Onley and Patience Wait, "Other agencies could benefit from NMCI's hard-learned lessons," Government Computer News [Online], 20 June 2005, 15 Apr. 2007 <http://www.gcn.com/print/24_15/36091-1.html>.

The Situation Pre-NMCI (late 1990s)

In the late 1990s, the Navy had 28 separate commands that budgeted and managed their own information technology (IT) systems and each command had an IT support staff. The shore establishment had almost 1,000 diverse networks operated and maintained by separate organizations, some of which could not e-mail each other, let alone collaborate. Among other problems, this limited the amount of reach-back for the forward forces, so that they could receive responsive logistical support. Furthermore, with close to 1,000 gateways, malicious intruders had many opportunities to exploit Navy networks. In 2001, the Navy experienced as many as 16,000 intrusions.[5]

Because of the diverse and heterogeneous nature of the resourcing and management of these IT systems, it was difficult for Navy and Defense officials to obtain visibility into how much was being spent, and how to improve management.

The Navy's Approach to Achieving an NMCI

Many large corporations in similar situations had merged their multiple networks into a single common one. The Navy, together with the Marine Corps, decided to follow the lead of companies such as IBM and FedEx and contract with industry to create a world-class, naval-wide intranet in a way that could keep up with the fast changing technology.

The Navy initiated the NMCI project in June 1999 and carried out six months of market research. The Navy decided to outsource the development and maintenance of a single, digital, secure, seamless network across the shore establishment to a single lead contractor in a fashion similar to the approach taken by many large corporations. The chosen approach was a performance-based services contract, also known as a “seat management” contract.

The Request for Proposal (RFP) was released December 23, 1999. To speed up the acquisition, the Navy did not define all of its technical requirements when it solicited contractor bids. Instead, it allowed the vendors to conduct their own site surveys at certain facilities and to develop their own proposals to achieve the desired capability without addressing thousands of technical specifications. The Navy also used the traditional approach of accepting questions from prospective bidders and providing written answers. This approach allowed the Navy to award NMCI quicker, but it deferred many of the driving technical issues until after the award.[6] One of these issues was the upgrade of legacy applications to meet the requirements for inclusion in NMCI.

---

[5] Charles L Munns, “A global Navy needs a global network,” US Naval Institute Proceedings 129.1, Jan. 2003: 60-62.

[6] Bill Murray, “The devil is in the details," Federal Computer Week [Online], 19 Mar. 2001, 1 Oct. 2004, <http://www.fcw.com/fcw/articles/2001/0319/mgt-devil-03-19-01.asp>.

The contract was awarded to EDS on October 6, 2000. The value of the contract including the 7-year base and 3-year option was $8.8B. Under the contract, EDS is responsible for providing all IT hardware and software, operations, training, maintenance, and system upgrades. The Navy is charged a fixed monthly price per user ("seat") throughout the life of the contract, provided EDS meets the specified service levels. The contract was one of the largest desktop outsourcings ever carried out, and the largest federal IT contract ever awarded. The 3-year option was exercised in March 2006.[7]

The contract includes incentives based on both Service Level Agreements (SLAs) and customer satisfaction surveys. There are currently 23 SLAs containing about 51 performance categories. Typical categories are Network Problem Resolution, NMCI Intranet Availability, and Latency/Packet Loss. In order to be paid the full amount allowed under the contract, a seat at a specific site must meet 100 percent of the applicable SLAs for that seat, as well as better than 50 percent of the seats at the site must be operational.

Customer satisfaction surveys are taken quarterly of end users who have 45 days or more of experience with NMCI. The contract stipulates that if there is 85 percent user satisfaction, EDS will receive $12.50 per seat per quarter for that organization. If the satisfaction is 90 percent, incentives increase to $25 per seat per quarter. In October 2004 two more customer categories were added, commanders and network operators, with surveys every 6 months. Additional incentives are based on these surveys. [For more detail on both performance and customer satisfaction incentives, see the 2006 GAO Report.[8]]

It is interesting to note that the Air Force and National Aeronautics and Space Administration (NASA) did not take the same approach as the Navy. The Air Force has said that NMCI makes sense for the Navy but not the Air Force. Air Force Col. William Cooper noted, "From our perspective, what the Navy did was to outsource what they do at fixed stations. The Navy doesn't fight from a fixed station; they fight from the fleet. The Air Force fights from fixed stations, and we rely too much on fixed stations to outsource it as a whole."[9]

NASA carried out 10 individual procurements at each of its 10 centers. The NASA organization is more decentralized than the Navy's and the culture and mission at each of the 10 centers is different. NASA also allowed the users to stay with the applications and operating systems they already were using.[10]

---

[7] "Navy/Marine Corps Intranet," Wikipedia, updated 30 March 2007, <http://en.wikipedia.org/wiki/Navy/Marine_Corps_Intranet>.
[8] U.S. Government Accountability Office, 2006.
[9] Bill Murray, and George Seffers, "Air Force won't follow NMCI lead," Federal Computer Week 15.5, 5 Mar. 2001: 16.
[10] Bill Murray, "There's more than one way to outsource," Federal Computer Week [Online], 19 Mar. 2001, 1 Oct. 2004, < http://www.fcw.com/fcw/articles/2001/0319/mgt-devsb-03-19-01.asp>.

The Promise of NMCI

The vision of NMCI was to consolidate Navy and Marine Corps computer networks into a single, secure, enterprise-wide managed service to include voice, video, and data. As such, NMCI held out the promise that anyone on the network would be able to communicate, collaborate, and exchange data with anyone else and that communication would be rapid and seamless. Figure 1 depicts the overall framework for the NMCI architecture.[11]

The goal of this consolidation was both to improve capabilities provided to each of the seats and reduce costs as a result of streamlined management and increased efficiencies. Figure 2 shows the overall NMCI concept and the projected improved capabilities and efficiencies to be achieved by its implementation.[12] The homogeneous enterprise network was intended to provide users with much improved performance over the previous heterogeneous, disparate set of networks.

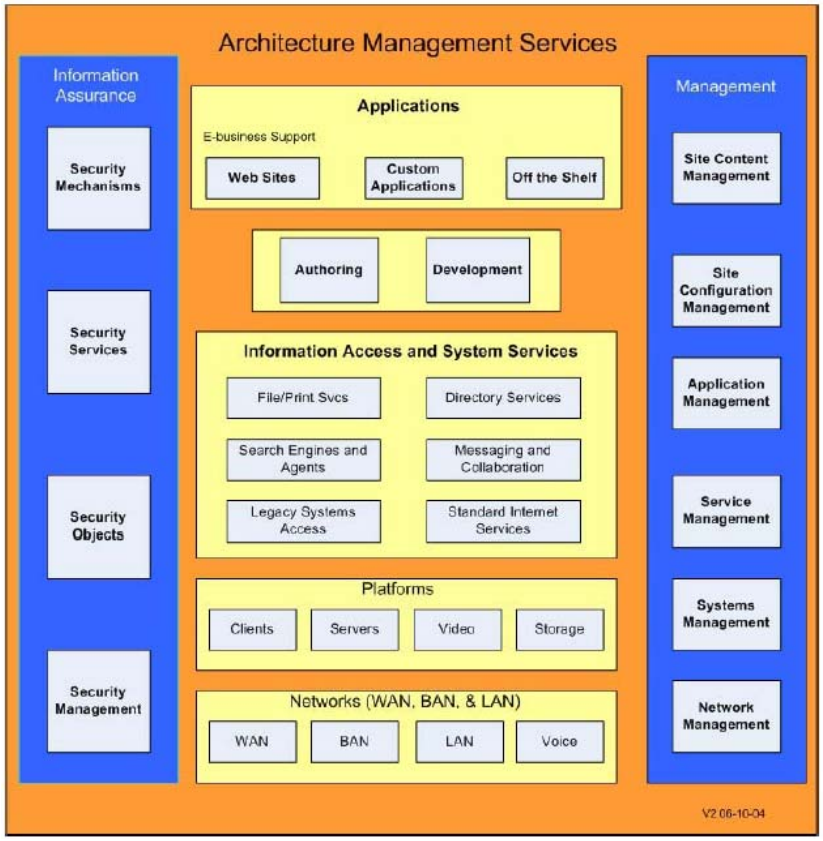

Figure 1. NMCI Architecture Framework

[11] NMCI Program Office, NMCI Release Development and Deployment Guide (NRDDG), 11 Oct. 2004, 19 Nov. 2004, <http://www.nmci.navy.mil/Primary_Areas/AppDevForum/Files/NRDDGs01.pdf>.
[12] RADM Charles L. Munns, Naval Studies Board-Enterprise IT-Precursor to FORCENet, Naval Studies Board Meeting, National Academy of Sciences, Washington DC, 22 Oct. 2003.

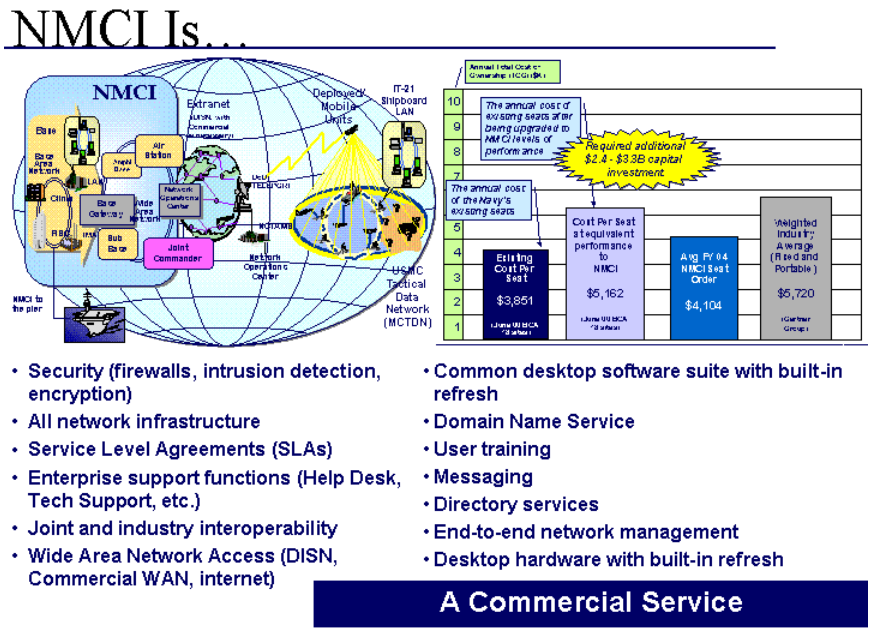

Figure 2. NMCI Concept and Improved Capabilities and Efficiencies

The centralized enterprise support, including tech support and help desk, replaced the large number of local tech support centers with a centralized contractor team and help desk, thus saving many manpower spaces and providing more responsiveness to user needs and in resolving network problems. By using standardized hardware, the Navy was to gain efficiencies in maintenance and repair, and the training of technicians.

The application of proven standardized security approaches including firewalls, intrusion detection, and encryption, as well as rigid security standards for applications aim to provide a highly secure network environment.

Gateways to Wide Area Networks (WAN), such as the Global Information Grid (GIG), Commercial WAN, and internet, as well as the Navy and Marine tactical networks provide users with the total connectivity needed to carry out their day-to-day work as well as their military missions.

User training was meant to be far simpler with standardized hardware and software because users would require little additional training as they moved around the enterprise.

NMCI would keep up with the rapid pace of technology by refreshing hardware every three years and providing software never more than one revision removed from the latest.

Problems Experienced in Implementation

Some of the early problems experienced by the program were the result of the fact that neither EDS nor the Navy fully understood the magnitude of the effort required to carry out the implementation of NMCI. This was, at least in part, due to the streamlined acquisition approach used by the Navy. Many of the driving technical requirements were not dealt with until after contract award. In March 2000, the GAO issued a report expressing deep concern about the Navy's risky acquisition approach. It concluded that "the Navy has developed and issued its request for proposals without developing a formal analysis of program alternatives and completing a business case analysis**,** to determine an appropriate acquisition strategy for the proposed Intranet."[13]

The rate of implementation of seats was initially lower than planned. This was especially true for the Marine Corps. At the 2004 NMCI Industry Symposium, Lt. Gen. Edward Hanlon, Commanding General of the Marine Corps Combat Development Command, commented,[14] "At Quantico, we recognized early that we had a problem. We were supposed to receive a delivery of 30 seats a day, but after the first 90 days of implementation, only 568 had been delivered." He also said, "I believe that EDS was not prepared to execute the implementation" and suggested that NMCI was under resourced at EDS.[15] This was clearly true, since EDS was losing money on NMCI, experiencing a $334M loss in the first quarter of 2003,[16] and a loss of $316M for the first six months of 2004.[17]

Underestimating the effect of the transition of legacy systems was a serious problem for NMCI and EDS. The goal for NMCI was to have 500 NMCI accredited, common user applications. It was recognized that EDS and the Navy would have to deal with legacy applications to be transitioned to reside on NMCI. It was initially assumed that the number of these applications was in the thousands. After contract award, the Navy and EDS were shocked to find the number was actually 100,000.[18] Since then, there has been an intensive effort to reduce that number to 3,000. As of late 2004, they had been successful at reducing them to only 31,000.[19]

---

[13] U.S. Government Accountability Office, Defense Acquisitions: Observations on the Procurement of the Navy/Marine Corps Intranet, GAO/T-NSIAD/AIMD-00-116, 8 Mar. 2000, <http://www.gao.gov/archive/2000/n100116t.pdf>.

[14] LtGen Edward Hanlon, Luncheon Speech, 2004 NMCI Industry Symposium, 22 Jun. 2004, 19 Nov. 2004,<http://www.nmci.navy.mil/Primary_Areas/Symposiums_Meetings/2004_NMCI_Industry_Symposium/Proceedings/uploads/hanlonNMCISPEECH.pdf>.

[15] Dawn Onley, "Hanlon on NMCI: 'EDS was not prepared,'" Washington Technology [Online], 22 Jun. 2004, 1 Oct. 2004, <http://www.washingtontechnology.com/news/1_1/enterprise-architecture/23853-1.html>.

[16] Michael Hardy, "EDS dealing with NMCI strain," Federal Computer Week [Online], 18 Jun. 2003), 1 Oct. 2004, <http://www.fcw.com/fcw/articles/2003/0616/web-eds-06-18-03.asp>.

[17] Bob Brewin, "England: NMCI on satisfying track," Federal Computer Week [Online], 17 Sep. 2004, 1 Oct. 2004, <http://www.fcw.com/fcw/articles/2004/0913/web-england-09-17-04.asp>.

[18] This number includes all versions of a single application that were actively being used.

[19] RADM Charles L. Munns, "NMCI-The DON Perspective," 21 Jun. 2004, 2004 NMCI Industry Symposium, 19 Nov.

The technology readiness of some aspects of NMCI was not adequate. An example is the required 500,000+ network node directory services that had not been previously attempted or tested. NMCI ended up as Microsoft Active Directory's research and development (R&D) test bed.[20]

Security has been another headache for NMCI and EDS, primarily driven by the legacy applications, but also from the cultural side of the effect on user convenience of policy enforcement. In order to have a smooth running, secure network, the security team must know which ports and protocols the applications use to communicate, so that when viruses or malicious visitors enter the network, they can be tagged as errant.[21] With many of the legacy applications being out of date or home grown and undocumented, EDS had to find ways to test the applications to obtain the needed information. This is part of the reason for the delays and overruns mentioned above.

Generally, NMCI has been successful in protecting the network from intrusions. They had a problem in 2003, when the network was successfully infiltrated by the Welchia worm. By late 2004, according to CAPT Christopher, staff director of NMCI, no infections had occurred and the system had detected and quarantined 563,182 viruses.[22] According to CAPT Christopher, the Naval Network Warfare Command (NETWARCOM) Red Team also failed to infiltrate the network.

One of the major problems the NMCI program had to deal with was the change in culture from a local oriented set of networks to a common, enterprise-wide solution. Users who were used to designing their own desktop, using their own logos, and being able to install their own applications in addition to the common applications were now no longer able to do that. They had to conform to stringent sets of rules, forgo installing applications of their choosing, and depend on enterprise management to load, maintain, and upgrade NMCI certified applications. Furthermore, the new security measures that were put in place tended, at least initially, to slow the system response time, causing much user unhappiness.

The SLAs embodying a large number of criteria turned out to be overly complex and difficult to manage. In some cases, the terms did not provide sufficient incentives to meet requirements. EDS often opted to fail SLAs and suffer the 15 percent penalty instead of suffering the much larger expenses to meet the SLA requirements.[23] The Navy subsequently negotiated to substantially reduce the number of criteria.

2004,<http://www.nmci.navy.mil/Primary_Areas/Symposiums_Meetings/2004_NMCI_Industry_Symposium/Proceedings/uploads/ADMMunns.ppt>.

[20] Rigano, 2007.

[21] Joab Jackson, "EDS secures NMCI with Securify: network monitoring tool helps identify many legacy applications," Washington Technology 18.13, 29 Sep. 2003: 25, <http://www.washingtontechnology.com/news/18_13/emerging-tech/21768-1.html>.

[22] William McMichael, "Intranet shows progress, but user's headaches persist," Federal Times 40.25, 2 Aug. 2004: 10.

[23] Rigano, 2007.

User dissatisfaction was significant. The main complaints were with the slow dial-up performance, limitations on size of file downloads (5-6Mbytes), and inability to personalize the programs on their computers. NMCI reported that according to the June 2004 survey, 75 percent of users were satisfied with the network, compared to 69 percent for the previous quarter and 60 percent for the last quarter of 2003.[24,25,26]

The Present Status

Positives

The Navy and Marine Corps have a secure, "enterprise-wide" network.[27]
The large number of disparate legacy networks has been replaced by single network. The following is a quote from the Navy comments to the 2006 GAO report on NMCI (included as an appendix to the report).[28] "With over 650,000 users now supported, NMCI has become the largest corporate intranet in the world. NMCI has consolidated over 1,000 legacy Department of the Navy (DoN) networks into a single, secure common computing and communications backbone with a standardized set of hardware and software across the enterprise. NMCI has deployed over 320,000 seats at hundreds of locations, all served by a world-class IT infrastructure."

The NMCI has been very secure, experiencing very few intrusions.
One clear advance that NMCI has made over the legacy systems is in network security. In response to the 2006 GAO report[29], the Navy claimed that "NMCI has never suffered a root-level intrusion and has thwarted attacks that penetrated other DOD systems on several occasions. NMCI is the only network that completely implemented and enforced the DOD's Public Key Infrastructure Cryptographic Log-On mandate. Every day NMCI strips more that 4,000 potentially harmful attachments from e-mails. In 2005, NMCI detected and countered over 2 million unauthorized intrusion attempts. NMCI provides a previously unavailable 'fail-over' capability, the ability to re-route during contingency operations and a centralized Network Operations Center to maintain 24/7 surveillance of network availability."

DoN capability to have visibility into IT expenditures and measure IT performance and customer satisfaction has considerably improved.
The introduction of a single, homogeneous, enterprise network with centralized reporting and control and customer surveys has allowed the DoN much improved visibility into IT expenditures, performance, and customer satisfaction.

---

[24] Matthew French, "Users getting comfortable with NMCI," Federal Computer Week 18.16, 24 May 2004: 54.
[25] Margaret Reed, "NMCI claims 75 percent satisfaction," Federal Computer Week [Online], 5 Aug. 2004, 1 Oct. 2004, <http://www.fcw.com/fcw/articles/2004/0802/web-nmci-08-05-04.asp>.
[26] Margaret Reed, "NMCI's silent majority," Federal Computer Week 18.28, 16 Aug. 2004: 72.
[27] With "enterprise" defined here as the fixed shore establishment.
[28] U.S. Government Accountability Office, 2006.
[29] U.S. Government Accountability Office, 2006.

Negatives

EDS has lost $3B and may not get it all back.

In the early years of the contract, as a result of the difficulties described earlier, EDS lost as much as $800M a year. According to EDS Chief Executive Officer (CEO) Michael Jordan, they are now achieving a positive cash flow, although he said that it is unlikely to turn a profit over its life span. “Three billion has been dissipated. We won't get it all back, but we will get a good percentage.”[30]

NMCI does not include the tactical edge.

Although the original objective was to seamlessly connect to the ship borne networks and the deployed forces, this connection is tenuous at best. Deployed forces, although they may have NMCI equipment, find that the equipment does not support their mission, and they have to carry out work-arounds using other equipment.[31]

Large file attachments (>5 MBytes), as well as Zip files are not allowed.

For reasons of performance, large files (>5MB) are prohibited. For reasons of security, Zip files (which could compress some of the large files) are not allowed because Zip files could contain malicious mobile code. For some Communities of Interest (COIs), this entails a negative operational impact on their missions.

NMCI tends to be segmented, not really an intranet.

For reasons of either security or perhaps the way the contract was set up, communication between members of some communities are limited. For example, a member of the Navy staff cannot share attachments with a Marine user. Neither user can share attachments with users in the medical community.[32]

New requirements are slow to be introduced.

New engineering requirements are required to go through quarterly cycles. It may be several cycles before solutions are fielded.[33]

NMCI does not meet the needs of all COIs.

Different COIs have different needs depending on their missions. For example, a COI involved in a short, but time urgent mission may wish to forego some security in favor rapid performance. NMCI does not allow this; it is a “one size fits all” solution. Similarly, three standardized desktops may not satisfy all of the 650,000 users. This is the source of some of the user dissatisfaction.

Legacy networks and applications are still prevalent.

Many commands are still using legacy networks and applications to an extent. Some of the reasons relate to the previously mentioned problems, and no overall strategy exists to

---

[30] Stan Gibson, "EDS Swabs the Decks of NMCI Mess,"eWeek.com [Online], 22 Jan. 2006), 15 Apr. 2007,< http://www.eweek.com/article2/0,1895,1914231,00.asp>.

[31] Rigano, 2007.

[32] Rigano, 2007.

[33] Rigano, 2007.

resolve these issues. There are contractual issues relating to who pays for legacy application and server hosting.[34]

Customer satisfaction is still below target.
The 2006 GAO report specifically investigated NMCI user satisfaction.[35] It found that the end user satisfaction rate is approximately 74 percent, below the target of 85 percent. It also found that operational users (commanders and network operators) had a much lower satisfaction rate. The user surveys have come under fire as to their objectivity.[36] They are controlled by the program office and the contractor and details are not released (some details are proprietary).

NMCI provides limited responsiveness to users' dynamic needs.
The loss of local IT support personnel has degraded responsiveness in maintaining and managing the network. The remote help desk is understaffed and do not understand the local problems. The government has limited visibility and control of network operations and management.

Lessons Learned

Although there are differing opinions about the success of NMCI, there is universal agreement on at least two items. First, the acquisition process has been difficult on both the government and contractor sides. Second, user satisfaction is not what it should be. From this experience, some lessons learned have been gleaned that may be useful both for other agencies embarking on a similar road, as well as for developing the strategy for the next generation NMCI, which is in progress. Sources that have been used in developing these lessons are the GCN article[37] and informal discussions with those working on the requirements process for the future NMCI.[38]

Forced commonality across the enterprise may not be the correct solution for half a million users in different COIs with differing requirements.
Different communities with different missions will generally have differing requirements profiles and these can change with time and circumstances. It has been noted that some tactical users have not been able to use NMCI for some of their missions and have had to resort to work-arounds. Users with time urgent missions may not be able to live with the time delays that may result from stringent security solutions. The enterprise network needs to have sufficient flexibility to accommodate these differences. It appears that this may be the source of much of the user dissatisfaction.

NMCI may well have been too large an effort for a single vendor.
There may be a limit as to how much can be outsourced to a single vendor, especially for this type of "seat management" contract. The opinion of a former officer in the Navy

[34] Rigano, 2007.
[35] U.S. Government Accountability Office, 2006.
[36] Wikipedia, 2007.
[37] Onley & Wait, 2005.
[38] Rigano, 2007.

Program Executive Office for IT is to go "for a more regional approach with multiple vendors."[39] Air Force Lt. Gen Charles Croom, Director of the Defense Information Systems Agency (DISA), has said in congressional testimony that the way to avoid such problems in the future is to "chop that problem up into smaller chunks, prototype and test before delivering larger chunks."[40]

The Navy spent insufficient time in the pre-contractual phase understanding its legacy infrastructure and applications and understanding the user's needs.
Neither the Navy nor the contractor sufficiently understood what they faced in transitioning from the legacy infrastructure and especially the number of legacy applications that had to be modified for security to work in the NMCI environment. Much more time should have been spent up front understanding the situation. An EDS executive was quoted as saying "With a contract the size of NMCI on the commercial side, the company would have spent six months of due diligence, and the contract would not be signed until due diligence is completed."[41]

At a hearing a congressional hearing in March 2007, Assistant Secretary of Defense for Networks and Information Integration (ASD NII) John Grimes said, "the user was not brought in when they were developing the system."[42]

The approach to replace local IT support personnel with centralized management and remote help desks may have gone too far.
Some of the user dissatisfaction stems from the poor responsiveness in dealing with network issues. Some issues are local in nature and can be better and more quickly be resolved at the local level. COIs should have their own network management capability and support; centralized managers may not understand what is needed at the COI level. The best solution is, more than likely, a mix of both approaches.

How NMCI fits in between the national and tactical systems was never clear.
The architectural relation of NMCI to the GIG and the tactical edge is not clear. Is NMCI duplicative of the GIG? Does NMCI include the tactical edge or just connect to it? It was stated that it did not include shipboard networks, but does it include other deployable nets? If not, how does it connect? These are issues that should be addressed in the next generation NMCI.

[39] Onley & Wait, 2005.
[40] Mark A. Kellner, "Officials Review NMCI Glitches, Lessons Learned,"DefenseNews.com [Online], 2 Apr. 2007, 1 May 2007, <http://defensenews.com/story.php?F=2657075&C=landwar>.
[41] Onley & Wait, 2005.
[42] Kellner, 2007.

Question 1. How would the NMCI program have been different if a different contractual approach had been used?

Better due diligence in the pre-contractual phase. It appears that neither the Navy nor the winning contractor had a sufficiently accurate understanding of the legacy problem before contract award. The pressures to move forward forced a highly compressed timeframe, which delayed a thorough investigation of the key issues of the legacy applications and the associated security challenges. There seems to be an indication that the winning contractor had not carried out sufficient site surveys and had a poorer understanding of the situation than the other competitors, and therefore bid a lower price and won. An approach involving several months of due diligence may have avoided this problem and provided a more level playing field. A better understanding on the part of the government would have given it a better foundation for proposal evaluation.

Phased, evolutionary approach. Perhaps a phased approach would have been better, starting with a smaller pilot program, using prototyping for example, and later increasing the scope after the major issues are better understood.

Single provider vs. multiple providers. NMCI is one of the largest efforts of its kind and the largest federal IT contract ever awarded. Perhaps it was too large for a single contractor. Also, once the contract was awarded, the Navy was locked in; there was no more competition. Would it have been better to divide NMCI up into smaller segments and start off with a number of contractors, then later down-select to the most efficient, effective providers, each dealing with one of the segments? This would have maintained competition and avoided the "single point failure" problem. The challenge here is that the Government must provide for the integration across contractors, keeping them coordinated and synchronized.

Question 2. Was the approach of outsourcing a large single homogeneous network the only way to achieve transformation to net centricity?

Basically, the NMCI is a single point solution to meeting the needs of groups of users (communities of interest) who have varying needs. That means that some users will find the solution wanting. Today, for example, some tactical users have the NMCI equipment, but do not use it because NMCI performance does not meet their needs. Would it make more sense to divide the overall network into segments, each meeting the needs of a group of users? Interoperability would then be provided, for example, by gateways between the segments. Each segment would be provided a level of performance within the segment, and another level provided across segments. As mentioned above, different contractors could be assigned the different segments.

Question 3. How does NMCI fit into the big picture architecture?

It has never been clear how NMCI fits into the total DOD architecture embodied in the Global Information Grid (GIG). Although the scope of the GIG is not particularly well defined, even at the DOD level, it basically supports the information needs at the national level and interfaces with the tactical networks of the Services. How does the NMCI fit into this picture? Does it overlap with the GIG? Does it overlap with the tactical networks? Or is it distinct from these networks and just interfaces with them? Could a better understanding of this avoid duplication and superfluous activity and provide a better functioning overall system?

Question 4. Where does the Department of the Navy go from here?

The present NMCI contract ends in 2010. What happens after that is not defined at this time, although there is activity defining the requirements and the approach to the Next Generation NMCI. If nothing is done, of course, the Navy will have the NMCI equipment and a network approach, but no contractor to manage it. Once the Next Generation NMCI is defined, there will have to be an arrangement for a (hopefully) seamless transition. Should considerations such as discussed above in Questions 1, 2, and 3 be dealt with in defining the follow-on and transition?